

GPG in 10 minutes

Shakthi Kannan, shaks_wants_no_spam_at_shakthimaan_dot_com

January 5, 2007

Revision: 1.2

Abstract

This documentation provides the basic usage of GPG: creating, importing, exporting, and submitting keys to key servers. Use your distro package manager to install GNU Privacy Guard (GPG). It will be installed by default in most recent distributions.

1 GPG Basic Usage

1.1 Creating keys

```
gpg --gen-key
```

It will ask lot of questions to create the key. You can use the default values. Remember your passphrase.

1.2 Exporting keys

```
gpg --armour --export "Tom Cruise <tom.cruise@e-mail.com>" > \
pubkey.asc
```

Your public key is pubkey.asc. You can check the current keys present using:

```
gpg --list-keys
```

A sample output:

```
~/ .gnupg/pubring.gpg
-----
pub   1024D/1644B902 2007-01-02
uid           Tom Cruise <tom.cruise@e-mail.com>
sub   2048g/4A7258D9 2007-01-02
```

The keyID is 1644B902.

1.3 Submitting keys to keyserver

To submit keys to a keyserver, say, pgp.mit.edu, do:

```
gpg --keyserver pgp.mit.edu --send-key 1644B902
```

1.4 Searching for keys

You can search for keys using:

```
gpg --keyserver pgp.mit.edu --search-keys "Tom Cruise"
```

1.5 Importing keys

To import keys to your pubring, you can do:

```
gpg --import whoispubkey.asc
```

1.6 Signing documents

To sign a document to send it to say, katie.holmes@e-mail.com, use the `-encrypt` option. You must have Katie Holmes' public key in your pubring.

```
gpg --output doc.gpg --encrypt --recipient \  
katie.holmes@e-mail.com document
```

As Katie Holmes, if you want to decrypt the above message, you can do:

```
gpg --output document --decrypt doc.gpg
```

It will ask for your passphrase.

1.7 Clearsign

You can also clearsign the document to be sent, via e-mail, for example, use:

```
gpg --clearsign document
```

The document contents will be embedded between the PGP signed message, as shown below:

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1  
  
[-----document-content-----]  
  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v0.9.7 (GNU/Linux)  
Comment: For info see http://www.gnupg.org  
  
iaYEA3ECAbyFA2dY3Qo4Cgk2J916UL31dqz4IwC5Q7wP6j/i81hbcwSK4rLyQB1  
oCoAo0wqpaqEfr4e0ksqHeLE/r8/Ra2k  
=y3k2  
-----END PGP SIGNATURE-----
```

2 Bibliography

- Brenno** . Brenno J.S.A.A.F. de Winter. August 10, 2004. Gnu Privacy Guard (GnuPG) Mini Howto (English). http://www.dewinter.com/gnupg_howto/english/GPGMiniHowto.html.
- David** . David R. Aspinall. Instant GPG HOWTO. <http://homepages.inf.ed.ac.uk/da/id/gpg-howto.shtml>.